I 05 (08/01/2005) (OM 07/28/2005

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 3

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Justin T. Darrow
Attorney Docket No.r	44424162-8724

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Class/Subclass Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
JD		4,211,919 A	07/08/1980	Michel Ugon	235/487
JD		4,295,041 A	10/13/1981	Michel Ugon	234/487
JD		4,916,333 A	04/10/1990	Jacek Kowalski	307/296.5
JD		4,932,053 A	06/05/1990	Serge Fruhauf et al.	380/4
JD		5,297,201 A	03/22/1994	John H. Dunlavy	380/6
JD		5,412,723 A	05/02/1995	Ran Canetti et al.	380/21
JD		5,636,157 A	06/03/1997	James H. Hesson et al.	364/700
JD		5,991,415 A	11/23/1999	Adi Shamir	380/30
JD		6,434,238 B1	08/13/2002	David Chaum et al.	380/45
JD		6,698,662 B1	03/02/2004	Nathalie Feyt et al.	235/492

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Class/Subclass Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
JD		~~EP 90201136.0~~ EP 0 399 587 A1	11/28/1990	Koninklijke PTT Nederland N.V.	H04L 9/06	☐
JD		WO 99/08411 A2	02/18/1999	Jonathan Stiebel	H04K 1/00	☐

Examiner Signature	Justin Darrow	Date Considered	08/2/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	09/930,836
				Filing Date	August 15, 2001
				First Named Inventor	Paul C. Kocher
				Group Art Unit	2132
(use as many sheets as necessary)				Examiner Name	Justin T. Darrow
Sheet	2	of	3	Attorney Docket No.	44424162-8724

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
JD		BACK, Adam, "Non-Interactive Forward Secrecy" 09/06/1996	
JD		BELL, Jim, "Spread-Spectrum Computer Clock?" Google Beta Groups	
JD		BELLARE et al., "Optimal Asymmetric Encryption", Advanced Networking Laboratories, 1998, pp 92-111, Springer-Verlag, U.S.A.	
JD		BELLARE et al, "The Exact Security of Digital Signatures- How to Sign with RSA and Rabin", Advances in Cryptology - Eurocrypt 96 Proceedings, Lecture Notes in Computer Science, Vol. 1070, , pp 1-16, U. Maurer ed., Springer-Verlag, 1996	
JD		BELLARE et al, "Forward Integrity For Secure Audit Logs", pp 1-16, November 23, 1997, U.S.A.	
JD		FRANKEL et al., "Optimal-Resilience Proactive Public-Key Cryptosystems" IEEE Symposium on Foundations of Computer Science, 1997	
JD		FRANKEL et al., "Proactive RSA", Lecture Notes in Computer Science, 1996	
JD		HERZBERG et al, "Proactive Public Key and Signature Systems", ACM Conference on Computer and Communications Security, 1996	
Examiner Signature	Justin Darrow	Date Considered	08/21/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 3 of 3

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Justin T. Darrow
Attorney Docket No.	44424162-8724

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
JD		MENZES et al, "Pseudorandom Bits and Sequences", Handbook of Applied Cryptography, CRC Press, Chapter 5, pp 169-190, 1996	
JD		MENZES et al, "Efficient Implementation", Handbook of Applied Cryptography, CRC Press, Chapter 14, pp 591-634, 1996	
JD		RIVEST, Ronald, "Timing Cryptanalysis of RSA, DH, DDS" Google Beta Groups	

Examiner Signature	Justin Darrow	Date Considered	08/21/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

IDS (05/02/2005) Com 04/28/2005

OIPE
MAY 0 2 2005
PATENT & TRADEMARK OFFICE

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Justin T. Darrow
Attorney Docket Number	44424162-8724

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Class/Subclass ~~Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear~~
JD		4,799,258 A	01-17-1989	Donald Davies	380/21
JD		5,506,905 A	04-09-1996	Dale Markowski et al.	380/25
JD		5,546,463A	08-13-1996	Anthony A. Caputo et al.	380/25

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Class/Subclass ~~Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear~~	T[6]
JD		EP 0 656 708 A1	06-07-1995	International Business Machines Corporation	H04L 9/08	☐
						☐

Examiner Signature	Justin Darrow	Date Considered	08/21/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Please type a plus sign (+) inside this box ™ +

PTO/SB/08B (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Justin T. Darrow
Attorney Docket Number	44424162-8724

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
JD		KOCHER, P., "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", 08/18/1996 XP000626590	

Examiner Signature	Justin Darrow	Date Considered	08/21/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.

IDS (01/05/2005) Corr. 12/31/2004

JAN 05 2005

PATENT AND TRADEMARK OFFICE

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Darrow, Justin T.
Attorney Docket Number	44424162-8724

U.S. PATENT DOCUMENTS

Class/Subclass

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
JD		4,211,919 A	07/08/1980	Ugon	235/487

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
						☐

Examiner Signature	Justin Darrow	Date Considered	08/21/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IDS (12/27/2004) Com 12/21/2004

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for ~~form~~ 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Darrow, Justin T.
Attorney Docket Number	44424162-8724

U.S. PATENT DOCUMENTS

Class/Subclass

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	~~Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear~~
JD		5,944,833 A	08/31/1999	Ugon	713/400

FOREIGN PATENT DOCUMENTS

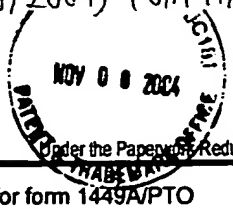
Class/Subclass

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	~~Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear~~	T[6]
JD		EP0826169B1	12/9/1997	Ugon	G06F 1/04	
JD		EP1064752B1	23/09/1999	Salle	H04L 9/06	
JD		EP1204948B1	1/2/2001	Leydier	G06K 19/073	
						☐

Examiner Signature	Justin Darrow	Date Considered	08/21/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

IDS(11/08/2004) (OM 11/03/2004



PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Darrow, Justin T.
Attorney Docket Number	44424162-8724

U.S. PATENT DOCUMENTS

Class/Subclass

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	~~Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear~~
JD		*5,664,017 A	09/02/1997	Gressel et al.	380/30

FOREIGN PATENT DOCUMENTS

Class/Subclass

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	~~Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear~~	T[6]
JD		EP 0 660 562 A2	6/28/1995	General Instrument Corporation of Delaware	H04L 9/00	☐
						☐

Examiner Signature	Justin Darrow	Date Considered	08/21/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IDS (10/05/2004) Com 09/30/2004

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Darrow, Justin T.
Attorney Docket Number	44424162-8724

U.S. PATENT DOCUMENTS

(GSI / Subclass)

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	~~Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear~~
JD	BT	4,107,458 A	01/08/1978	Constant	178/22
JD	BU	4,139,839 A	01/02/1979	~~Fletcher et al.~~ Engel et al.	340/347DD
JD	BV	4,569,052 A	04/02/1986	Cohn et al.	371/38
JD	BW	4,605,921 A	08/01/1998	Riddle et al.	340/347DD
JD	BX	5,144,667 A	09/01/1992	Pogue, Jr. et al.	380/45
JD	BY	5,159,632 A	10/27/1992	Crandell	380/28
JD	BZ	5,297,201 A	03/22/1994	Dunlavy	380/6
JD	CA	5,511,123 A	4/23/1996	Adams	380/29
JD	CB	5,551,013 A	08/27/1996	Beausoleil et al.	315/500
JD	CC	5,559,890 A	09/09/1996	Obermeire et al	380/48
JD	CD	5,670,934 A	09/23/1997	Ina et al.	340/426
JD	CE	5,710,834 A	01/01/1998	Rhoads	382/232
JD	CF	5,892,829 A	04/06/1999	Aiello et al.	380/25
JD	CG	5,982,900 A	11/09/1999	Ebihara et al.	380/30

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
						☐
						☐
						☐
						☐

Examiner Signature	Justin Darrow	Date Considered	08/21/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control no.

Please type a plus sign (+) inside this box ™ +

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Darrow, Justin T.
Attorney Docket Number	44424162-8724

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	CiteNo.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
JP	CH	LACY, J. et al., "CryptoLib Version 1.1", File Bigpow.c from CryptoLib, United States, November 1999.	
JP	CI	"File NN.C from RSAFEF", RSA Laboratories, a division of RSA Data Security, Inc., United States, 1991.	
JP	CJ	WAYNER, P., "Code Breaker Crack Smart Cards, Digital Safe", New York Times, United States, 06/22/98, on the World Wide Web at: http://www.nytimes.com/library/tech/98/06/biztech/articles/22card.html	

Examiner Signature	Justin Darrow	Date Considered	08/12/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.

IDS (08/13/2004) Com 09/10/2004

SEP 13 2004

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 4

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Darrow, Justin T.
Attorney Docket Number	44424162-8724

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Class / Subclass Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
JD	AA	US-4,200,770 A	04/29/1980	Hellman et al.	178/22
JD	AB	US-4,203,166 A	05/13/1980	Ehrsam et al.	375/2
JD	AC	US-4,211,919 A	07/08/1980	Ugon	235/487
JD	AD	US-4,214,126 A	07/22/1980	Wipff	179/1.5M
JD	AE	US-4,243,890 A	01/06/1981	Miller et al.	250/551
JD	AF	US-4,405,829 A	09/20/1983	Rivest et al.	178/22.1
JD	AG	US-4,759,063 A	07/19/1988	Chaum	380/30
JD	AH	US-4,905,176 A	02/27/1990	Schulz	364/717
JD	AI	US-5,136,643 A	08/04/1992	Fischer	380/23
JD	AJ	US-5,241,598 A	08/31/1993	Raith	380/21
JD	AK	US-5,297,201 A	03/22/1994	Dunlavy	380/6
JD	AL	US-5,341,423 A	08/23/1994	Nossen	380/6
JD	AM	US-5,369,706 A	11/29/1994	Latka	380/23
JD	AN	US-5,404,402 A	04/04/1995	Sprunk	380/14
JD	AO	US-5,412,379 A	05/02/1995	Waraska et al.	340/825.72
JD	AP	US-5,539,827 A	07/23/1996	Liu	380/37
JD	AQ	US-5,544,086 A	08/06/1996	Davis et al.	364/408
JD	AR	US-5,546,463 A	08/13/1996	Caputo et al.	380/25

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Class / Subclass Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	AS	EP 0 529 261 A2	03/03/1993	IBM Corp.	H04L 9/28	☐
	AT	EP 0 582 395 A2	02/09/1994	Digital Equipment Corp.	H04L 29/06	☐
						☐
						☐
						☐

Examiner Signature	Justin Darrow	Date Considered	08/2/12005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

SEP 13 2004

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 4

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Darrow, Justin T.
Attorney Docket Number	44424162-8724

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Class/Subclass Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
JD	AU	US-5,552,776 A	09/03/1996	Wade et al.	340/825.31
JD	AV	US-5,559,887 A	09/24/1996	Davis et al.	380/24
JD	AW	US-5,600,324 A	02/04/1997	Reed et al.	341/176
JD	AX	US-5,633,930 A	05/27/1997	Davis et al.	380/24
JD	AY	US-5,663,896 A	09/02/1997	Aucsmith	395/187.01
JD	AZ	US-5,733,047 A	03/31/1998	Furuta et al.	384/43
JD	BA	US-5,761,306 A	06/02/1998	Lewis	380/21
JD	BB	US-5,778,065 A	07/07/1998	Hauser et al.	380/21
JD	BC	US-5,848,159 A	12/08/1998	Collins et al.	380/30
JD	BD	US-5,991,415 A	11/23/1999	Shamir	380/30
JD	BE	US-5,995,629 A	11/30/1999	Reiner	380/50
JD	BF	US-6,041,122 A	03/31/2000	Graunke et al.	380/21
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
						☐
						☐
						☐
						☐
						☐

Examiner Signature	Justin Darrow	Date Considered	08/21/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449B/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	09/930,836
				Filing Date	August 15, 2001
				First Named Inventor	Paul C. Kocher
				Group Art Unit	2132
(use as many sheets as necessary)				Examiner Name	Darrow, Justin T.
Sheet	3	of	4	Attorney Docket Number	.44424162-8724

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	B G	BELLARE et al., "Incremental Cryptography: The Case of Hashing and Signing" in: DESMEDT, Y., Advances in Cryptology - Crypto '96 (Berlin, Springer, 1996), pp. 104-113	
	B H	MENZES et al., "Handbook of Applied Cryptography" (CRC Press, 1996), pages including 285-298, 312-319, 452-462, 475, 512-524	
	B I	Bank Technology News. "Cries of Wolf Over Smart Card Security?" Faulkner & Gray, Inc. 01 November 1996	
	B J	American National Standards for Financial Services, secretariat - American Bankers Association (ANS/ABA x9.24-1997), "Financial Services Key Management," approved April 6, 1992, American National Standards Institute; pgs. 1-71	
	B K	JUENEMAN, Robert R., "Analysis of Certain Aspects of Output Feedback Mode", Satellite Business Systems, 1998; pgs. 99-127	
	B L	BAUER, Friedrich L., "Cryptology - Methods and Maxims", Technical University Munich, 1998; pgs. 31-48	
	B M	CONNOR, Doug (Technical Editor), "Cryptographic Techniques - Secure Your Wireless Designs", 01/18/96; pgs. 57-68	
	B N	HORNAUER et al., "Markov Ciphers and Alternating Groups," Eurocrypt 91, 1991; pgs. 453-460	

Examiner Signature	Justin Darrow	Date Considered	08/21/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Substitute for form 1449B/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	09/930,836
				Filing Date	August 15, 2001
				First Named Inventor	Paul C. Kocher
				Group Art Unit	2132
(use as many sheets as necessary)				Examiner Name	Darrow, Justin T.
Sheet	4	of	4	Attorney Docket Number	44424162-8724

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
JD	BO	KOBLITZ, "A Course in Number Theory and Cryptography" 2e, 1994, Chapter III; pgs. 53-77	
JD	BP	LAI et al., "Markov Ciphers and Differential Cryptanalysis," Eurocrypt 91, 1991; pgs. 17-38	
JD	BQ	HACHEZ et. al. "Timing Attack: What Can Be Achieved By A Powerful Adversary?" 1999	
JD	BR	KOCHER, Paul C., "Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attacks," Report 7 December 1995; pgs. 1-6	
JD	BS	KALISKI, Burt, "Timing Attacks on Cryptosystem," RSA Laboratories, Bulletin, Number 2, January 23, 1996	

Examiner Signature	Justin Darrow	Date Considered	08/21/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.